10-11-05

Walker & Jocke
a legal professional association

Ralph E. Jocke
Patent
&
Trademark Law

October 6, 2005

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re:	**Application Serial No.:**	**10/648,936**
	Appellants:	**Steinmetz, et al.**
	Filing Date:	**August 27, 2003**
	Confirmation No.:	**5940**
	Title:	**AUTOMATED BANKING MACHINE CONFIGURATION SYSTEM AND METHOD**
	Docket No.:	**D-1150 DIV**

Sir:

Please find enclosed the Brief of Appellant pursuant to 37 C.F.R. § 41.37 for filing in the above-referenced application.

Please charge the fee required with this filing ($500) and any other fee due to Deposit Account 09-0428 of Diebold Self-Service Systems.

Very truly yours,

Ralph E. Jocke
Reg. No. 31,029

CERTIFICATE OF MAILING BY EXPRESS MAIL

I hereby certify that this document and the documents indicated as enclosed herewith are being deposited with the U.S. Postal Service as Express Mail Post Office to addressee in an envelope addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 7th day of October, 2005

EV715375627US
Express Mail Label No.

Ralph E. Jocke

330 • 721 • 0000 MEDINA | 330 • 225 • 1669 CLEVELAND | 330 • 722 • 6446 FACSIMILE | rej@walkerandjocke.com E-MAIL

231 South Broadway, Medina, Ohio U.S.A. 44256-2601

D-1150 DIV

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	**Richard A. Steinmetz, et al.**	)	
		)	Art Unit
Serial No.:	**10/648,936**	)	**3624**
Confirm. No.:	**5940**	)	
Filed:	**August 27, 2003**	)	Patent Examiner
		)	**Lalita M. Hamilton**
For:	**Automated Banking Machine Configuration System and Method**	)	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS PURSUANT TO 37 C.F.R. § 41.37

Sir:

The Appellants hereby submit their Appeal Brief pursuant to 37 C.F.R. § 41.37 concerning the above-referenced Application.

10/12/2005 BABRAHA1 00000110 090428 10648936
01 FC:1402 500.00 DA

(i) REAL PARTY IN INTEREST

The Assignee of all right, title and interest to the above-referenced Application is Diebold, Incorporated, an Ohio corporation.

(ii) RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and the assignee of the present application are not aware of any other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF CLAIMS

Claims 13-24 and 28-34 are pending in the Application.

Claims rejected: 13-24 and 28-34

Claims allowed: none

Claims confirmed: none

Claims withdrawn: none

Claims objected to: none

Claims canceled: 1-12 and 25-27

Appellants appeal the rejections of claims 13-24 and 28-34. These claim rejections were the only claim rejections present in the Office Action ("Action") dated May 24, 2005, which was made non-final. Claims 13-24 have been twice rejected.

(iv) STATUS OF AMENDMENTS

A non-final rejection was made May 24, 2005. No amendments to the claims were requested to be admitted after the non-final rejection.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

Concise explanations of exemplary forms of the claimed invention:

With respect to independent claim 13

An exemplary form of the invention is directed to a method for configuring an automated banking machine (146) (Figure 6). As discussed in the Specification at page 1, line 10 to page 2 line 2, a common type of automated banking machine is an automated teller machine ("ATM") which enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries.

The method comprises a step (a) of receiving a certificate (150, 160) (Figures 6 and 7) through operation of the banking machine (Page 5, line 21 to page 6, line 2; page 17, line 20 to page 18 line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

The method further comprises a step (b) of authenticating at least one digital signature associated with the certificate through operation of the banking machine (page 12, lines 6-11). Examples discussed in the Specification for this step include configuration software (148) operating the ATM (146) which is operative to authenticate the certificate (150) using digital signature authentication techniques (Page 24, line 17 to page 25, line 5).

In addition the method comprises a step (c) of configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b) (page 25, lines 5-7). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17 to page 26, line 12).

With respect to independent claim 24

Another exemplary form of the invention is directed to computer readable media bearing instructions (148) (Figure 6) which are operative to cause a computer in an automated banking machine (146) to carry out method steps. As discussed in the Specification at page 1, line 10 to page 2 line 2, a common type of automated banking machine is an automated teller machine ("ATM") which enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries.

Such method steps include a step (a) of receiving a certificate (150, 160) (Figures 6 and 7) through operation of the banking machine (Page 5, line 21 to page 6, line 2; page 17, line 20 to page 18 line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

The method further comprises a step (b) of authenticating at least one digital signature associated with the certificate through operation of the banking machine (page 12, lines 6-11). Examples discussed in the Specification for this step include configuration software (148) operating the ATM (146) which is operative to authenticate the certificate (150) using digital signature authentication techniques (Page 24, line 17 to page 25, line 5).

In addition the method comprises a step (c) of configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b) (page 25, lines 5-7). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17 to page 26, line 12).

With respect to independent claim 28

Another exemplary form of the invention is directed to a method for configuring a cash dispensing automated teller machine (ATM) (10, 148) (Figures 1, and 6). As discussed in the Specification at page 1, line 10 to page 2 line 2, an ATM enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries.

The method steps include a step (a) of receiving at least one digitally signed certificate (150, 160) (Figures 6 and 7) through operation of the ATM (Page 5, line 21 to page 6, line 2; page 17, line 20 to page 18 line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

In addition the method is directed to an ATM which includes a cash dispenser (20) and at least one processor. In addition, the method is directed to at least one certificate which includes at least one serial number (Page 26, line 10) which is also referred to in the specification as a hardware embedded value.

The method further comprises a step (b) of verifying through operation of the at least one processor that the at least one serial number or hardware embedded value included in the at least one certificate corresponds to at least one serial number or hardware embedded value associated with at least one hardware device of the ATM (Page 27, 19 to page 28, line 1).

In addition, the method comprises a step (c) of, responsive to step (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate (Page 28, 1-2). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17 to page 26, line 12).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds to be reviewed in this appeal are:

Whether Appellants' claims 13-24 and 28-34 are anticipated under 35 U.S.C. § 102(b) by Dulude, et al., U.S. Patent No. 6,310,966 ("Dulude").

(vii) ARGUMENT

Dulude

Dulude is directed to a system that authenticates users using biometrics in combination with digital certificates (Column 3, lines 39-50). The system includes biometric certificates (16) which include biometric data (20) therein (Figure 2). The biometric data is pre-stored as biometric certificates in a biometric database (66) of a biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device (26) (Figure 3). Subsequent transactions to be conducted over a network (60) have transaction biometric data (46) generated from the physical characteristics of the current user, which is then appended to transaction first data (50), and which then authenticates the user by comparison against the pre-stored biometric data of the physical characteristics of users in the biometric data base (Figures 4 and 5).

A second classifier (84) generates a decision in the form of a second validation signal (86), which may be a logic value indicating verification of the authenticity of the user sending the electronic transaction. The second validation signal may also be a numeric value corresponding to a percentage of confidence of authenticity (Figure 5, Column 7, lines 58-67). A receiving section (42) may respond to the validation signals (82, 86) to process the transaction first data (50) such as an on-line purchase or an electronic funds transfer (Column 8, lines 1-7).

Although Dulude mentions that ATMs may access the memory of a smart card to obtain a biometric certificate of a user (Column 5, lines 45-49), Dulude does not teach how ATMs use such certificates. Dulude only discloses using certificates to authenticate users. Thus, Dulude may arguably suggest that an ATM obtain a biometric certificate of a user for purposes of

authenticating the user. However, nowhere does Dulude disclose or suggest any other use for biometric certificates other than to authenticate users. As will be discussed below in more detail, Appellants claims are not directed to using certificates to authenticate users. Rather, Appellants' claims are directed to using certificates to configure an automated banking machines such as ATMs. Nowhere does Dulude disclose or suggest using its biometric certificates or any other type of certificates to configure an ATM or anything else.

The 35 U.S.C. § 102 (b) Rejections

The Applicable Legal Standards

Anticipation pursuant to 35 U.S.C. § 102 requires that a single prior art reference contain all the elements of the claimed invention arranged in the manner recited in the claim. *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Anticipation under 35 U.S.C. § 102 requires in a single prior art disclosure, each and every element of the claimed invention arranged in a manner such that the reference would literally infringe the claims at issue if made later in time. *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987).

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used

or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999).

It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

Rejection under 35 U.S.C. § 102(b) over Dulude

Claims 13-24 and 28-34 were rejected under 35 U.S.C. § 102(b) as being anticipated by Dulude. These rejections are respectfully traversed.

Claim 13

Claim 13 is an independent claim directed to a method for configuring an automated banking machine. The Action states that Dulude discloses a method and corresponding program comprising configuring an automated banking machine (Page 2). Applicants disagree. Nowhere in Column 5, lines 30 to column 7, line 45 or anywhere else does Dulude disclose or suggest a method for configuring an automated banking machine.

Further, claim 13 recites "configuring the banking machine responsive to the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to a certificate. Dulude is directed to a system that authenticates users using biometric certificates. Nowhere does Dulude disclose or suggest that its biometric certificates are used by an automated banking machine to configure the automated banking machine. Further, nowhere

does Dulude disclose or suggest any feature or data in its biometric certificates that is capable of being used to configure an automated banking machine.

Further claim 13 recites configuring the banking machine responsive to the certificate and "authentication of the at least one digital signature associated with the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to both a digital certificate and authentication of a digital signature associated with the certificate.

In addition claim 13 recites authenticating at least one digital signature associated with the certificate through operation of the banking machine. Dulude does not disclose an automated banking machine that operates to authenticate a digital signature associated with its biometric certificates.

The Action's assertions are not based on any evidence in the record. An assertion of prior art knowledge not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, supra. The determination of patentability must be based on evidence of record. *In re Lee*, supra. Appellants respectfully submit that because the rejection is based on mere assertions and not proper evidence of record, it is not a valid rejection.

Dulude does not explicitly or inherently teach the recited features, relationships, and steps. For all of these many reasons Dulude does not anticipate claim 13. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(b) rejection should be withdrawn.

Claim 14

Claim 14 depends from claim 13. Dulude does not disclose or suggest that a digital signature included in a certificate is authenticated responsive to a public key of a licensing

authority through operation of an automated banking machine. Dulude does not explicitly or inherently teach this feature and therefore does not anticipate claim 14.

Claim 15

Claim 15 depends from claim 13. Dulude teaches that software may be used to append transaction biometric data (46), transaction first data (50), and a digital signature (58) (Column 6, lines 18-26). However, nowhere does Dulude disclose or suggest that a certificate corresponds to at least one software component. In addition, nowhere does Dulude disclose or suggest that a certificate corresponds to at least one software component authorized to be installed on an automated banking machine. Further, nowhere does Dulude disclose or suggest installing at least one software component on an automated banking machine. Also, Dulude does not disclose or suggest installing at least one software component corresponding to the certificate on an automated banking machine. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 15.

Claim 16

Claim 16 depends from claim 13. Dulude teaches generating a biometric certificate from a set (16) of data that includes a subject unique ID (18), and biometric data (20) (Column 4, lines 7-8). However nowhere does Dulude disclose or suggest a certificate which includes a plurality of sets of configuration rules. Further, nowhere does Dulude disclose or suggest that each set of configuration rules corresponds to at least one of a plurality of automated banking machines. In addition nowhere does Dulude disclose or suggest that an automated banking machine is enabled

to be configured responsive to at least one set of the configuration rules included in a digital certificate. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 16.

Claim 17

Claim 17 depends from claim 13. Dulude teaches that authenticating certificates in the prior art may be generated by concatenating a message and a public key with a set of data which may include an expiration of validity of the certificate (Column 1, line 66 to column 2, line 9). However, nowhere does Dulude disclose or suggest determining through operation of an automated banking machine responsive to the expiration parameter in a certificate that configuration of software on the machine is not authorized. In addition, Dulude does not disclose or suggest determining through operation of an automated banking machine responsive to the expiration parameter in a certificate that configuration of software on the machine is not authorized. Further nowhere does Dulude disclose or suggest preventing configuration of software on the banking machine. In addition, nowhere does Dulude disclose or suggest preventing configuration of software on the banking machine responsive to the determination that configuration of software on the machine is not authorized. As Dulude does not explicitly or inherently teach these features, Dulude does not anticipate claim 17.

Claim 18

Claim 18 depends from claim 13. Dulude teaches that authenticating certificates in the prior art may be generated by concatenating a message and a public key with a set of data (Column 1, line 66 to column 2, line 13). However, nowhere does Dulude disclose or suggest that a set of data included in a certificate includes an identification value unique to the banking machine. As the Dulude does not explicitly or inherently teach this feature, Dulude does not anticipate claim 18.

Claim 19

Claim 19 depends from claim 18. Nowhere does Dulude disclose or suggest determining through operation of the banking machine that the identification value included in the certificate corresponds to a hardware embedded identification value in the banking machine. Dulude does not explicitly or inherently teach this feature and therefore does not anticipate claim 19.

Claim 20

Claim 20 depends from claim 13. Nowhere does Dulude disclose or suggest a certificate which includes a terminal identification value. Further nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to the certificate including associating the machine with the terminal identification value. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 20.

Claim 21

Claim 21 depends from claim 20. Nowhere does Dulude disclose or suggest determining that the terminal identification value has changed. Further nowhere does Dulude disclose or suggest preventing the machine from performing at least one transaction function responsive to the determination that the terminal identification value has changed. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 21.

Claim 22

Claim 22 depends from claim 13. Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, nowhere does Dulude disclose or suggest retrieving the certificate from a licensing authority through operation of an automated banking machine. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 22.

Claim 23

Claim 23 depends from claim 13. Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, nowhere does Dulude disclose or suggest receiving the certificate from a server in operative connection with the banking machine. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 23.

Claim 24

Claim 24 is an independent claim directed to computer readable media. Nowhere does Dulude disclose or suggest computer readable media bearing instructions which are operative to cause a computer in an automated banking machine to carry out method steps. Claim 24 further recites that these method steps include "configuring the banking machine responsive to the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to a certificate. Dulude is directed to a system that authenticates users using biometric certificates. Nowhere does Dulude disclose or suggest that its biometric certificates are used by an automated banking machine to configure the automated banking machine. Further, nowhere does Dulude disclose or suggest any feature or data in its biometric certificates that is capable of being used to configure an automated banking machine. Further, nowhere does Dulude disclose or suggest computer readable media bearing instructions which are operative to cause a computer in an automated banking machine to configuring the banking machine responsive to the certificate.

Further claim 24 recites that the method steps include configuring the banking machine responsive to the certificate and "authentication of the at least one digital signature associated with the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to both a digital certificate and authentication of a digital signature associated with the certificate. Further, nowhere does Dulude disclose or suggest computer readable media bearing instructions which are operative to cause a computer in an automated

banking machine to configure the banking machine responsive to the certificate and authentication of the at least one digital signature associated with the certificate.

In addition claim 24 recites authenticating at least one digital signature associated with the certificate through operation of the banking machine. Dulude does not disclose an automated banking machine that operates to authenticate a digital signature associated with its biometric certificates. Further, nowhere does Dulude disclose or suggest computer readable media bearing instructions which are operative to cause a computer in an automated banking machine to authenticating at least one digital signature associated with the certificate.

The Action's assertions are not based on any evidence in the record. An assertion of prior art knowledge not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, supra. The determination of patentability must be based on evidence of record. *In re Lee*, supra. Appellants respectfully submit that because the rejection is based on mere assertions and not proper evidence of record, it is not a valid rejection.

Dulude does not explicitly or inherently teach the recited features, relationships, and steps. For all of these many reasons Dulude does not anticipate claim 24. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(b) rejection should be withdrawn.

Claim 28

Claim 28 is an independent claim directed to a method for configuring a cash dispensing automated teller machine (ATM). Nowhere does Dulude disclose or suggest a method for configuring a cash dispensing ATM.

Dulude teaches that an authenticating certificate in the prior art may include a serial number for the certificate with respect to a sequence of generated certificates (Column 2, lines 6-8). However, nowhere does Dulude disclose or suggest verifying through operation of at least one processor in an ATM that the at least one serial number included in at least one certificate received by the ATM corresponds to at least one serial number associated with at least one hardware device of the ATM. Further, nowhere does Dulude disclose or suggest that any other data included in a certificate corresponds to a serial number associated with an ATM hardware device.

In addition, claim 28 recites "responsive to (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate." Nowhere does Dulude disclose or suggest configuring an ATM responsive to a certificate. Dulude is directed to a system that authenticates users using biometric certificates. Nowhere does Dulude disclose or suggest that its biometric certificates are used by an ATM to configure the ATM. Further, nowhere does Dulude disclose or suggest any feature or data in its biometric certificates that is capable of being used to configure an ATM. Also nowhere does Dulude disclose or suggest configuring an ATM responsive to a step (b) of verifying that at least one serial number included in a certificate corresponds a serial number associated with an ATM hardware device.

The Action's assertions are not based on any evidence in the record. An assertion of prior art knowledge not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, supra. The determination of patentability must be based on evidence of record. *In re Lee*, supra. Appellants respectfully submit that because the rejection is based on mere assertions and not proper evidence of record, it is not a valid rejection.

Dulude does not explicitly or inherently teach the recited features, relationships, and steps. For all of these many reasons Dulude does not anticipate claim 28. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(b) rejection should be withdrawn.

Claim 29

Claim 29 depends from claim 28. Dulude does not disclose or suggest authenticating the at least one digital signature included in the certificate through operation of the at least one processor in an ATM. In addition, Dulude does not disclose or suggest configuring an ATM responsive to both authenticating the at least one digital signature included in the certificate and verifying that at least one serial number included in the certificate corresponds a serial number associated with an ATM hardware device. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 29.

Claim 30

Claim 30 depends from claim 29. Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, Dulude does not disclose or suggest receiving the at least one certificate with the ATM from a server in operative connection with the ATM through a network. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 30.

Claim 31

Claim 31 depends from claim 30. Nowhere does Dulude disclose or suggest configuring an ATM responsive to a step (b) of verifying that at least one serial number included in a certificate corresponds a serial number associated with at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device of an ATM. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 31.

Claim 32

Claim 32 depends from claim 30. Nowhere does Dulude disclose or suggest that prior to configuring the ATM responsive to the certificate, the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device and configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 32.

Claim 33

Claim 33 includes a typographical error with respect to the claim from which it depends. Claim 33 should depend from claim 32. Upon the resolution of the Appeal, Applicant is willing to correct claim 33 to depend from claim 32.

With respect to the subject matter recited in claim 33, nowhere does Dulude disclose or suggest that configuring the ATM responsive to a certificate includes enabling the ATM to

dispensing cash through operation of the cash dispenser in the ATM. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 33.

Claim 34

Claim 34 depends from claim 30. Nowhere does Dulude disclose or suggest configuring an ATM responsive to at least one key provided in the at least one certificate. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 34.

CONCLUSION

Each of Appellants' pending claims specifically recites elements, relationships, and steps that are neither disclosed nor suggested in any of the applied prior art. Furthermore, the applied prior art is devoid of any teaching, suggestion, or motivation for producing the recited invention. For these reasons it is respectfully submitted that all the pending claims are allowable.

Respectfully submitted,

Ralph E. Jocke Reg. No. 31,029
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000

(viii) CLAIMS APPENDIX

13. A method for configuring an automated banking machine comprising:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

14. The method according to claim 13, wherein in step (a) the certificate includes the digital signature, wherein in step (b) the digital signature is authenticated responsive to a public key of a licensing authority.

15. The method according to claim 13, wherein in step (a) the certificate corresponds to at least one software component authorized to be installed on the banking machine, and further comprising installing the at least one software component on the banking machine.

16. The method according to claim 13, wherein in step (a) the certificate includes a plurality of sets of configuration rules each set corresponding to at least one of a plurality of automated banking machines, and wherein in step (c) the banking machine is enabled to be configured responsive to at least one set.

17. The method according to claim 13, wherein the certificate further includes an expiration parameter, and further comprising:

d) determining through operation of the banking machine responsive to the expiration parameter that configuration of the software on the machine is not authorized; and

e) preventing configuration of software on the banking machine responsive to the determination in step (d).

18. The method according to claim 13, wherein in step (a) the certificate includes an identification value unique to the banking machine.

19. The method according to claim 18, further comprising prior to step (c):

determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine.

20. The method according to claim 13, wherein in step (a) the certificate includes a terminal identification value, wherein step (c) includes associating the machine with the terminal identification value.

21. The method according to claim 20, further comprising:

d) determining that the terminal identification value has changed; and

e) preventing the machine from performing at least one transaction function responsive to the determination in step (d).

22. The method according to claim 13, wherein step (a) includes retrieving the certificate from a licensing authority.

23. The method according to claim 13, wherein step (a) includes receiving the certificate from a server in operative connection with the banking machine.

24. Computer readable media bearing instructions which are operative to cause a computer in an automated banking machine to carry out the method steps of:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

28. A method for configuring a cash dispensing automated teller machine (ATM) comprising:

a) receiving at least one digitally signed certificate through operation of the ATM, wherein the ATM includes a cash dispenser and at least one processor, wherein the at least one certificate includes at least one serial number;

b) verifying through operation of the at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM;

c) responsive to (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate.

29. The method according to claim 28, wherein the at least one certificate includes at least one digital signature; and further comprising:

d) prior to (c) authenticating the at least one digital signature through operation of the at least one processor;

wherein (c) is carried out responsive to (b) and (d).

30. The method according to claim 29, wherein (a) includes receiving the at least one certificate from a server in operative connection with the ATM through a network.

31. The method according to claim 30, wherein the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device.

32. The method according to claim 30, wherein prior to (c) the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device, wherein in (c) configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device.

33. The method according to claim 33, wherein in (c) the at least one transaction function includes dispensing cash, wherein further comprising:

e) dispensing cash from the ATM through operation of the cash dispenser.

34. The method according to claim 30, wherein (c) includes configuring the ATM responsive to at least one key provided in the at least one certificate.

(ix) EVIDENCE APPENDIX

(None)

(x) RELATED PROCEEDINGS APPENDIX

(None)